

⑫ 公開特許公報(A)

昭63-229541

⑪ Int.Cl.⁴

識別記号

庁内整理番号

⑬ 公開 昭和63年(1988)9月26日

G 06 F 12/14

3 1 0

C-7737-5B

審査請求 有 請求項の数 5 (全4頁)

⑭ 発明の名称 データ交換システム

⑯ 特 願 昭63-47338

⑰ 出 願 昭63(1988)2月29日

優先権主張 ⑱ 1987年3月4日 ⑲ 西ドイツ(DE) ⑳ P3706957.8

㉑ 発 明 者 デイートリツヒ、クル ドイツ連邦共和国オットーブルン、ウルメンシュトラーセ
ーゼ 9㉒ 発 明 者 アルブレヒト、ボイテ ドイツ連邦共和国オットーブルン、シュワルベンシュトラ
ルシュバツヒアー ーセ78㉓ 発 明 者 アネツテガブリエル、 ドイツ連邦共和国ウイースバーデン、フラウエンロープシ
ケルステン ュトラーセ6㉔ 出 願 人 シーメンス、アクチエ ドイツ連邦共和国ベルリン及ミュンヘン(番地なし)
ンゲルシャフト

㉕ 代 理 人 弁理士 富 村 潔

明 細 書

1. 発明の名称 データ交換システム

2. 特許請求の範囲

- 1) 少なくとも1つのデータ入力/データ出力装置とチップカードの形態の少なくとも1つの携帯可能なデータ担体とを有するデータ交換システムであって、データ入力/データ出力装置およびチップカードがそれぞれ付属の制御およびアドレス指定回路を有する独立したプログラム可能なデータメモリと、それぞれマイクロプロセッサのなかに組み込まれている共通の真正確認アルゴリズムと、記憶されたそれぞれ等しい秘密キーとを備えているデータ交換システムにおいて、カスタマーカード(KK)としての役割をするチップカードが乱数発生器を含んでおり、その都度発生された乱数(v)がカスタマーカード(KK)のなかでもカスタマー端末器(KT)としての役割をするデータ入力/データ出力装置のなかに伝達後にもデータメモリからプログラ

ム(P)の一部をデータフロー制御のために選択し、これらのプログラム部分(Pv)から真正確認アルゴリズム(I)および秘密キー(KPC)を利用してそれぞれ真正確認コード(PACv)が計算され、またカスタマーカード(KK)のなかに比較装置(COM P)が設けられ、この比較装置が一方ではカスタマーカード(KK)のなかで計算された真正確認コード(PACv)および他方ではカスタマー端末器(KT)のなかで計算されかつカスタマーカード(KK)のなかに伝達された真正確認コード(PACv)の同一性を検査することを特徴とするデータ交換システム。

- 2) カスタマー端末器(KT)のなかで選択されたプログラム部分(Pv)が固有の安全モジュールのなかに伝達され、そのなかで真正確認コード(PACv)がそこに格納されている秘密コード(KPCs)およびそこに組み込まれている真正確認アルゴリズム(Is)

を利用して計算され、また計算された結果が直接にカスタムカード (KK) のなかの比較装置 (COPM) に伝達されることを特徴とする請求項1記載のデータ交換システム。

- 3) 安全モジュールが差し込みカード (SK) として構成されていることを特徴とする請求項1記載のデータ交換システム。
- 4) データフロー制御のためのプログラム (P) からのデータ (Pv) の選択が、各第kビットまたはバイトが選択されるように行われることを特徴とする請求項1ないし3の1つに記載のデータ交換システム。
- 5) プログラムデータ (Pv) の選択が、第1の乱数発生器の出力信号により始動される第2の乱数発生器により制御されることを特徴とする請求項1ないし3の1つに記載のデータ交換システム。

3. 発明の詳細な説明

(産業上の利用分野)

この発明は、少なくとも1つのデータ入力/デ

ータ出力装置とチップカードの形態の少なくとも1つの携帯可能なデータ担体とを有するデータ交換システムであって、データ入力/データ出力装置およびチップカードがそれぞれ付属の制御およびアドレス指定回路を有する独立したプログラム可能なデータメモリと、それぞれマイクロプロセッサのなかに組み込まれている共通の真正確認アルゴリズムと、記憶されたそれぞれ等しい秘密キーとを備えているデータ交換システムに関するものである。

最近のデータ処理および通信システムではデータの保護がますます重要な役割を演ずる。システムがデータ保護に関し十分な対策を施しているかどうかは、システムへのアクセスを正当な人に対してのみ可能にし、逆に不当な人を絶対的な安全性をもって締め出すことがどの程度に達成されているかどうかに関係する。システムへのアクセスの正当性を検査するための絶対的に安全ではないが簡単な方法は、たとえば、正当な利用

者によりのみ知られており、また利用者により任意に頻繁に変更できるいわゆるパスワードを使用する方法である。パスワードは、無資格者により探知または盗聴される危険があるので、補助的な安全対策が不可欠である。これらの対策の一つは、たとえば、伝達される情報の暗号化およびその解読であり、データ処理システムにおいてなかなかチップカードの利用によっても実現可能である対策である。

(従来の技術)

この発明は、少なくとも1つのデータ入力/データ出力装置とチップカードの形態の少なくとも1つの携帯可能なデータ担体とを有するデータ交換システムであって、データ入力/データ出力装置およびチップカードがそれぞれ付属の制御およびアドレス指定回路を有する独立したプログラム可能なデータメモリと、それぞれマイクロプロセッサのなかに組み込まれている共通の真正確認アルゴリズムと、記憶されたそれぞれ等しい秘密キーとを備えているデータ交換システムに関するものである。

ている。

別の安全対策手段はシステムに対するチップカードの真正確認を利用して構成され得る。この真正確認は、任意の加入者が正当であると虚偽の申し立てをすることによりシステム内の秘密情報にアクセスすることを防止する。真正確認のための重要な前提は加入者の個人別のコピー不可能な特徴である。加入者のこのコピー不可能な特徴は、両パートナー（すなわちチップカードとシステムの両者）に、一層詳細にはこれらの両パートナーにのみ知られている暗号化およびその解読のための秘密のキーを利用することにより得られる。

しかしながら、チップカードと利用者端末器との間の緊密な回路技術的結び付きは、チップカードの利用者のみとそのアイデンティティを証明するだけでなく、端末器の側でもデータフローが端末器内で操作されずに進行することが保証されていることをも前提とする。その例は、チップカード利用者により書込まれた識別番号PINが読出され得ないこと、また端末器により指示されたデ

ータがチップカードに伝達されたデータに一致することである。従って、利用者に真正らしいデータが指示されたり、またチップカード内で誤ったデータが処理されるような操作は絶対的な安全性をもって排除されなければならない。

(発明が解決しようとする課題)

本発明の課題は、冒頭に記載した種類のデータ交換システムを、利用者端末器内の操作不可能なデータフロー制御が保証されるように構成することである。

(課題を解決するための手段)

この課題は、本発明によれば、カスタマーカードとしての役割をするチップカードが乱数発生器を含んでおり、その都度発生された乱数がカスタマーカードのなかでもカスタマー端末器としての役割をするデータ入力/データ出力装置のなかに伝達後にもデータメモリからプログラムの一部をデータフロー制御のために選択し、これらのプログラム部分から真正確認アルゴリズムおよび秘密キーを利用してそれぞれ真正確認コードが計算さ

査される。この検査はクリプトグラフィックな方法により行われる。そのために、カスタマー端末器KTのメモリのなかに格納されている外部に対し秘密にすべきプログラム部分Pが個人化の際にカスタマーカードまたは検査用カードのなかに参照データとして記憶されることが必要である。さらに、カスタマー端末器KTにおける秘密キーKPCの確実な記憶が可能であることが前提とされている。さらに、カスタマーカードKKおよびカスタマー端末器KTの両者に共通の真正確認アルゴリズムIをが与えられている。この真正確認アルゴリズムIおよび秘密キーKPCを利用してプログラムデータからカスタマー端末器KTおよびカスタマーカードKKの両者において真正確認パラメータまたはプログラム真正確認コードPACvが計算される。偽造されたプログラムにもかかわらずプログラム真正確認コードPACvのコピーによる盗聴アクセスおよび操作を予防するため、乱数vを利用してダイナミックなプログラム検査が行われる。乱数vはカスタマーカードKKのな

れ、またカスタマーカードのなかに比較装置が設けられ、この比較装置が一方ではカスタマーカードのなかで計算された真正確認コードおよび他方ではカスタマー端末器のなかで計算されたカスタマーカードのなかに伝達された真正確認コードの同一性を検査することにより解決される。本発明の有利な実施態様は請求項2以下にあげられている。

(実施例)

以下、本発明の実施例を図面により一層詳細に説明する。

第1図には、左部にチップカードとして構成されたカスタマーカードKKが、また右部にいわゆるカスタマー端末器KTが示されており、それらのなかに本発明にとって主要な回路要素が形成されている。カスタマー端末器KTのなかにデータフロー制御のための正しいプログラムPが存在しているか否かは、個人識別番号PINの入力前にカスタマーカードKKにより、もしくはたとえば毎日の作業開始時に検査用チップカードにより検

査で発生され、さらにカスタマー端末器KTに伝達される。これにより乱数vに関して、カスタマーカードKKのなかでもカスタマー端末器KTのなかでも秘密なプログラム部分PからデータブロックPvが選択される(モジュールSELを参照)。従って、プログラム・真正確認コードPACvの前記の計算はこの選択されたデータブロックPvに基づいて関係式

$$PACv = I(KPC; Pv)$$

に従って行われる。計算された両プログラム・真正確認コードPACvの一方、詳細にはカスタマー端末器KTのなかで計算されたプログラム・真正確認コードが最終的にカスタマーカードKKに伝達され、そこでそこに設けられている比較装置COMPが、カスタマーカードKKにより計算された結果とカスタマー端末器KTにより計算された結果とが一致するかどうかを確認する。

カスタマーカードKKのなかにもカスタマー端末器KTのなかにも格納される秘密キーKPCの確実な記憶のためには2つの方法がある。第1の

方法は、秘密キーKPCを確実なプログラム可能な読み出しメモリのなかに格納する方法である。第2の方法では、キーKPCが特殊なチップカードからカスタマー端末器KTのカード読み取り装置を介してカスタマー端末器の書き込み・読み出しメモリのなかに読込まれる。このメモリに対する電流供給は外部から行われる。

真正確認アルゴリズム*f*としてワンウェイ・ファンクションが使用されると好適である。このアルゴリズムは、比較的容易にチップカードのなかに組み込まれるように、複雑さの少ないものでなければならない。

乱数*v*を利用して秘密プログラム部分PからデータブロックPvを選択するためには多くの方法が考えられる。たとえば各第*k*ビット/バイトがプログラム部分Pから選択されればよく、その際*k*は固定であり、また選択により開始されるべき乱数*v*を決定する。または*k*=*v*であり、また開始はプログラム部分Pの第1のビット/バイトで行われる。しかし、乱数*v*はたとえば出発値とし

て別の乱数発生器を始動させ、その出力信号が選択されたデータブロックPvに対するビット/バイトを決定してもよい。

チップカードKKのなかに秘密プログラム部分に対して過大なメモリ容量を必要としないように、記憶されたプログラム部分Pはカード固有であってもよい。それにもかかわらずカードの全体により、すべての秘密プログラム部分Pの検査が保証される。

端末器のなかに相異なるカードシステムを使用する際には、プログラム・真正確認コードPACvがカスタマー端末器KTではなく固有の安全モジュールにおいて、たとえば取扱者端末器における固有の安全カードSK(第2図参照)において検査されることによって、プログラム検査はシステムに無関係に行われ得る。カード提示者に、プログラム検査を行うべきか否か、またその仕方が任されている。特に、真正確認アルゴリズム*f*sおよび秘密キーKPCsは提示者により自由に選択可能である。この形態のプログラム検査の別の

利点は、秘密キーがカスタマー端末器KT内には記憶される必要がないことである。

4. 図面の簡単な説明

第1図は本発明によるデータ交換システムにおけるデータフローを検査するための回路装置のブロック図、第2図は第1図による回路装置の変形例のブロック図である。

KK…カスタマーカード

KT…カスタマー端末器

P…外部に秘密にすべきプログラム部分

KPC…秘密キー

f…真正確認アルゴリズム

PAC…プログラム・真正確認データ

v…乱数

Pv…選択されたデータブロック・プログラム部分

SEL…選択モジュール

COMP…比較装置

Sk…安全カード

*f*s…Sk内の真正確認アルゴリズム

FIG1

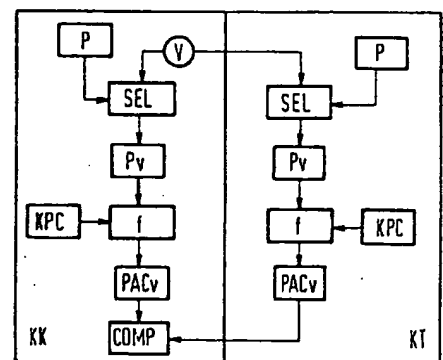


FIG2

